ZyXEL

Professional Integrated SSL-VPN Appliance for Small and Medium-sized businesses

- Clientless Secure Remote Access
- Seamless Integration behind the Existing Firewall Infrastructure
- UTM Security Integration Deployed Alongside ZyWALL UTM
- Supporting AD/LDAP/RADIUS and Two-factor Authentication
- ZyWALL SSL-VPN SecuExtender Technology
- Unified Policy Management with Object-Based Configuration
- Endpoint Security Support
- Dual-Mode (NAT-/DMZ-Mode) Installation with Setup Wizard

Integrated SSL-VPN Appliance

ZyWALL SSL 10

Benefits

Clientless Secure Remote Access

The ZyWALL SSL 10 is an integrated SSL-VPN appliance designed for small and medium-sized organizations with simple, secure and clientless remote access to the resources on corporate networks.

Remote access has never been so easy since no client software is required on users' laptops. They are enabled to access corporate applications or shared files with just standard Web browsers, no pre-installed or pre-configured VPN software is needed. Better yet, administrators can reduce the costly support tasks involved in deploying, configuring and updating VPN software.

Highly Integrated Capabilities on Existing Network Infrastructure

The ZyWALL SSL 10 fits seamlessly into any network topology and can be easily deployed alongside almost any third-party firewall as a secure remote access solution. This enables you to leverage the existing network infrastructure without the need to purchase additional hardware. When deployed alongside a ZyWALL UTM running Anti-Virus and IDP Service, the ZyWALL SSL 10 utilizes the powerful UTM technology to scan traffics for malicious threats such as viruses, worms, Trojans and spyware.

Comprehensive End-User Authentication Mechanism

The ZyWALL SSL 10 supports not only the internal database, but also various backend user repositories such as Microsoft Active Directory, LDAP and RADIUS to seamlessly integrate with the existing user database. ZyWALL SSL 10 supports the Two-factor Authentication method that requires two independent pieces of information to recognize identity and grant privileges. Two-factor Authentication is stronger and more rigorous than the traditional password authentication that requires only one factor (the user password), and it is especially useful for protecting against threats from keylogger programs.

ZyWALL-SSLVPN SecuExtender Technology

ZyWALL SSL 10 provides powerful capability to seamlessly access any corporate network resource by transparently pushing a downloadable thin client (ZyWALL-SSLVPN SecuExtender) to users' desktops or laptops. Administrators can allow specific user groups (such as employees) to create IPSec-like network tunnels for accessing any resource, while other user groups (such as customers, vendors or partners) may access restricted applications and resources listed only on the user portal.

Unified Policy Management with Object-Based Configuration

The ZyWALL SSL 10 provides the ability for administrators to define objects such as user groups, network address ranges or applications. When security policies are changed, administrators can modify the pre-defined objects and propagate the changes instantly without redefining rules, enabling businesses to implement and manage security policies easily and consistently.

For example, administrators can create one policy for the Sales group to access general applications, and create another for R&D to access confidential design documents in addition to the general elements.

Endpoint Security Support

Remote access enables more users to take advantage of the network from potentially risky end points and devices, including wireless hotspots and unmanaged PDAs; however the risk could render access management through user identity simply insufficient. To effectively control network access, ensure secure communications and reinforce data protection, more attention need to be paid to the security level of user environments.

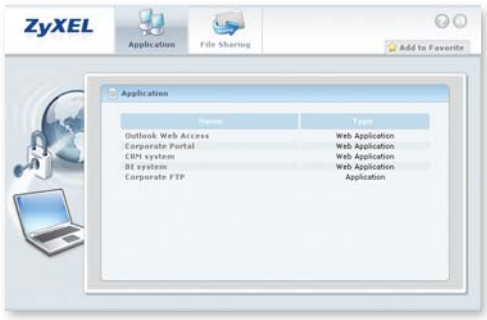
The ZyWALL SSL 10 provides endpoint security features to enhance protection by detecting the presence of required processes (e.g. virus scan, personal firewalls, OS patch levels, registry settings, etc.) on the client PC as well as the browser cache cleaner.

Dual-Mode (NAT-/DMZ-Mode) Installation with Setup Wizard

With the ability to shorten the initial setup procedure to less than 10 minutes, the two-scenario Setup Wizard helps administrators to easily configure the device and reduce the administration cost. The ZyWALL SSL 10 can be easily deployed at the network gateway as a one-box Firewall/SSL-VPN device, or alongside any third-party firewall as a secure remote access solution.

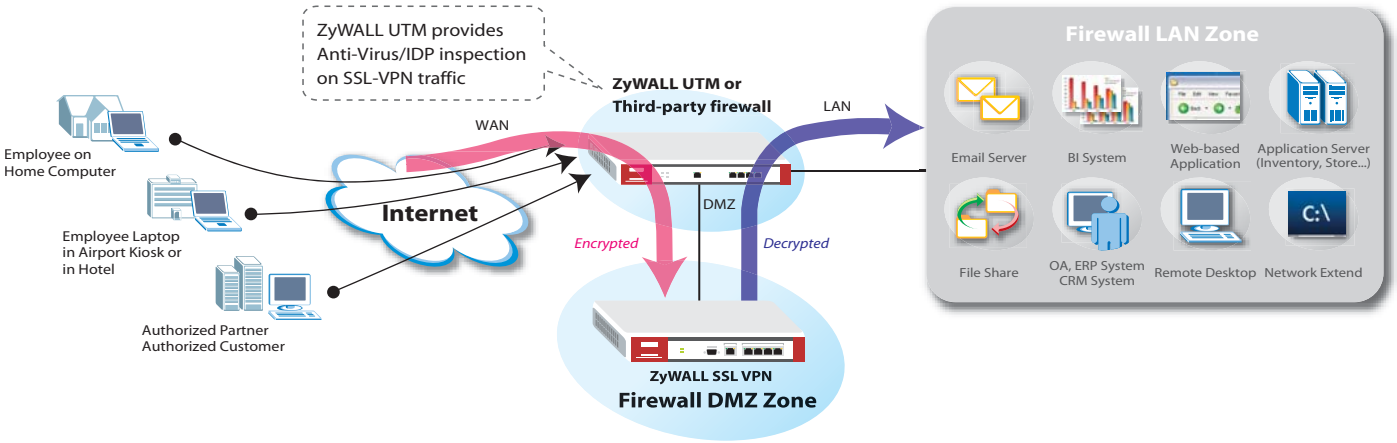
Clientless Secure Remote Access

- Using standard browser to access Internal network applications

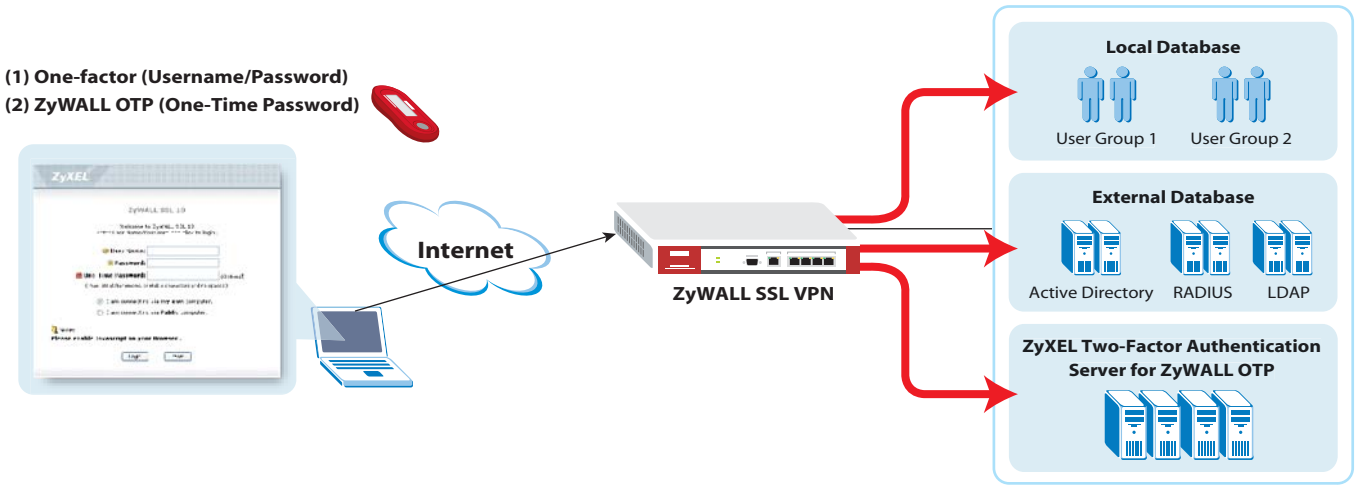


- Using standard browser to access Internal file-sharing folder

Highly Integrated Capabilities on Existing Network Infrastructure

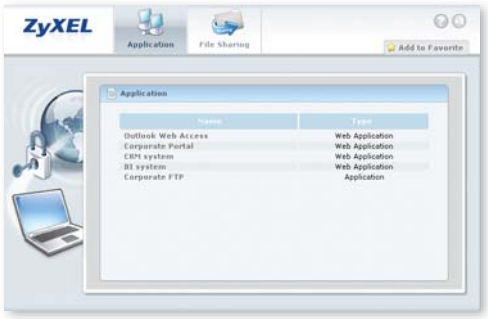


Comprehensive End-User Authentication Mechanism



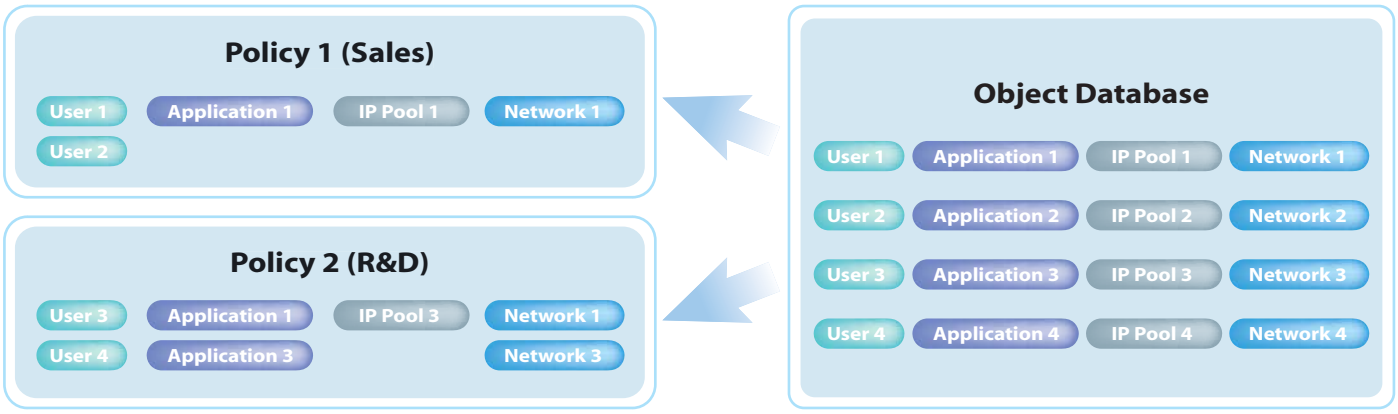
ZyWALL-SSLVPN SecuExtender Technology

- Restricted Access: Extranet Application for Partners, customers

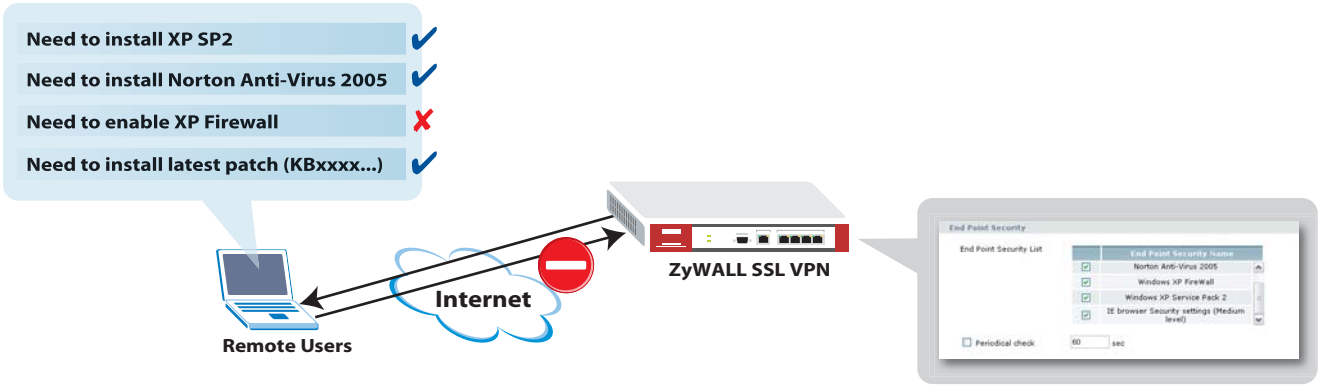


- Full Access: Intranet Application for Employees

Unified Policy Management with Object-Based Configuration



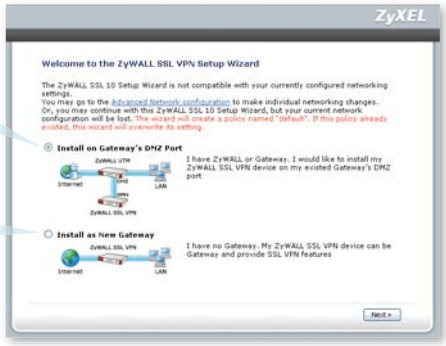
Endpoint Security Support



Dual-Mode (NAT-/DMZ-Mode) Installation with Setup Wizard

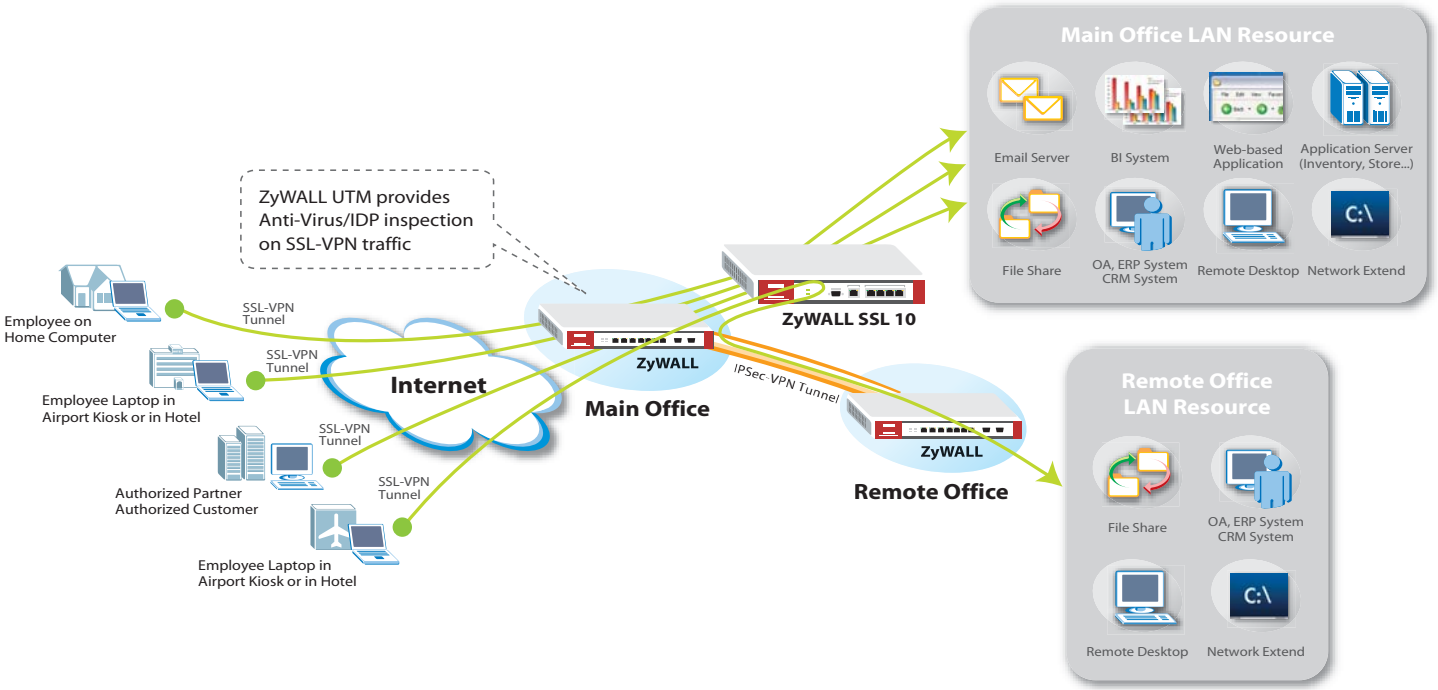
DMZ Mode:
Deployed behind Firewall (at DMZ port of Firewall)

NAT Mode:
Deployed at network gateway as one-box solution for NAT Router and SSL-VPN Gateway

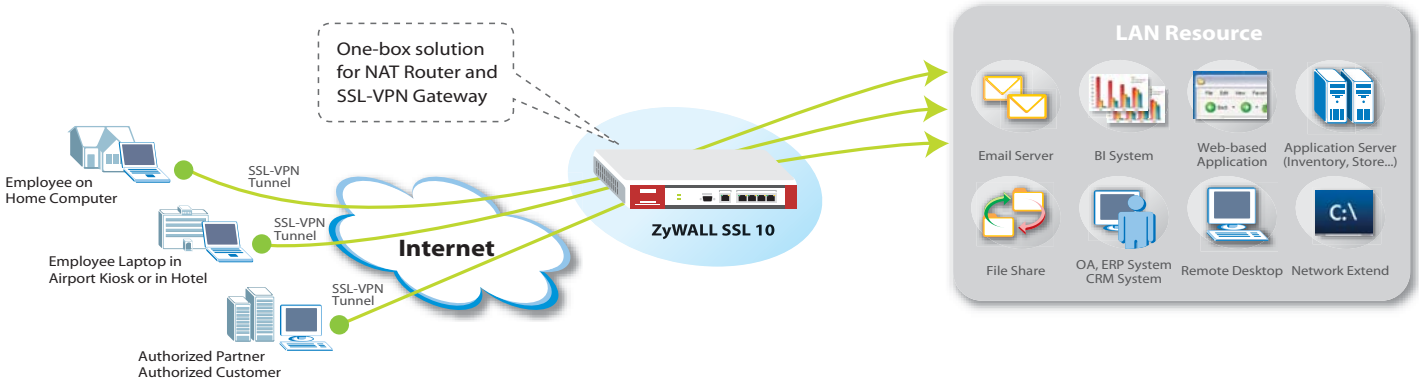


Application Diagram

DMZ Mode:
Deployed behind Firewall



NAT Mode:
Deployed at Network Gateway



For more product information, visit us on the web www.ZyXEL.com

Copyright © 2007 ZyXEL Communications Corp. All rights reserved. ZyXEL, ZyXEL logo are registered trademarks of ZyXEL Communications Corp. All other brands, product names, or trademarks mentioned are the property of their respective owners. All specifications are subject to change without notice.

65-100-002501G 02/07

Specifications

System Specifications

Mode of Deployment

- NAT Mode
- DMZ Mode

Networking

- WAN: PPPoE, Static, DHCP
- LAN: DHCP Server
- NAT

SSL VPN

- SSL VPN Tunnel: 10, 25 (Optional Upgrade)
- SSL Protocol: SSL v2, SSL v3, TLS 1.0
- Encryption: DES, 3DES, RC4 (128), AES (128, 256), IDEA, ADH, DH, DHE, RSA, DSS, CBC, 3CBC, MD5, SHA-1

SSL-VPN Access Mode

- Reverse Proxy Mode
- Port Forwarding Mode
- Full Tunnel Mode

Authentication

- Internal user database
- RADIUS
- LDAP
- Microsoft Active Directory
- Two-factor Authentication

Certification

- Self-signed
- External CA

Application Support

- Web Application: Web Server, Internet Email, OWA
- Non Web-based Application: HTTP, HTTPS, FTP, Telnet, TFTP, SMTP, SMTPS, IMAP, IMAPS, VNC, RDP, NTP, SSH, SQUID, CIFS, POP3, POP3S
- File-Sharing: Web-based CIFS
- Full Network Access via ZyWALL-SSLVPN SecuExtender: Any TCP/IP based application (ICMP, VoIP, IMAP, POP, SMTP, etc.)

Browser Support

- Internet Explorer version 5.5 with MSXML, version 6 and above.
- Netscape version 7.2 and above
- Mozilla 1.7.3 and above
- Firefox 1.0 and above

Security

- User-/Group-based Policy Control
- User-/Group-based Access Control
- User-/Group-based IP Pools
- User-/Group-based Routing
- User-/Group-based Application List
- User-/Group-based Endpoint Integrity Check
- Cache Cleaning

System Management

- Web GUI
- Dual-mode Setup Wizard
- Dashboard
- Email Notification
- Real-time Monitoring
- Logs
- Report
- NTP Support

Hardware Specifications

- Processor: 266 MHz with cryptographic accelerator
- Memory (Flash/DRAM): 128 MB/128 MB
- Status LED Indicator: PWR, SYS
- Reset Button: Yes
- WAN: 10/100 Auto MDI/MDIX
- LAN: 4-Port Switch, 10/100 Auto MDI/MDIX
- Console: RS 232 DB9 Connector
- Power: 12 VDC
- Max Power Assumption: 7.5 W
- Warranty: Two years

Physical Specifications

- Dimensions: 242.0 (W) x 75.0 (D) x 35.5 (H) mm
- Weight: 1,200 g

Environmental Specifications

- Operation Environment:
  - Temperature: 0°C ~ 50°C
  - Humidity: 20% ~ 95%
- Storage Environment:
  - Temperature: -30°C ~ 60°C
  - Humidity: 20% ~ 95%